GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2104.1A CHGE 1
May 3, 2016

GSA ORDER

SUBJECT: GSA Information Technology (IT) General Rules of Behavior

1. Purpose. This Order sets forth the General Services Administration's (GSA's) policy on IT General Rules of Behavior. The IT General Rules of Behavior implement the Federal policies and GSA Directives provided in the "References" section of this order.

2. Cancellation. This Order cancels CIO 2104.1 (July 3, 2003).

3. Objectives. The objectives of the IT General Rules of Behavior are to ensure that all authorized users of GSA IT resources are aware of their responsibilities and expected behavior in safeguarding those resources. GSA IT resources include hardware (computers, including desktops, laptops, mobile devices including Blackberries and smart phones, and storage devices, including USB/flash drives and portable external hard drives) as well as GSA or contractor provided software and systems. The Rules of Behavior apply to all resources that are used on the GSA network.

4. Applicability. This Order applies to all GSA service, staff office, and regional employees. As specified in their respective contracts or operating agreements, the requirements of this order also applies to contractors or other third parties who access GSA IT resources to conduct business on behalf of, or with, GSA or GSA supported Government organizations, and to all GSA IT resources which process or store GSA data, whether leased or owned. Owners/operators of contracted commercial IT resources/systems, not connected to GSA IT resources, must develop commercial IT system specific Rules of Behavior.

5. Explanation of change paragraph. Section 7, IT Rules of Behavior chart, Category: "Access," amended to add the following highlighted:

> "(3) Lock GSA systems with a PIN/password and remove PIV card when away from the work area, including for lunch, breaks, or any extended period of time."

6. References.

a. Appendix III, Office of Management and Budget (OMB) Circular A-130 – Security of Federal Automated Information Resources;

b. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq;

c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: the NIST Handbook;

d. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;

e. GSA Order CIO P2100.1, GSA IT Security Policy;

f. GSA Order CIO 2160.2, GSA Electronic Messaging and Related Services;

g. GSA Order CPO 1878.1, GSA Privacy Act Program;

h. GSA Order CIO 2100.3, Mandatory IT Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities;

i. GSA Order OGC 7800.11A ADM, Personal Use of Agency Office Equipment;

j. GSA Order CIO 2106.1, GSA Social Media Policy;.

k. GSA Instructional Letter, IL-12-01, Mobile Device Applications;

l. GSA Order CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

Refer to http://insite.gsa.gov/directives and http://csrc.nist.gov for the latest versions of these references.

7. Roles and responsibilities.

a. GSA Managers must:

(1) Ensure that authorized users, including GSA employees and contractors, who access GSA IT resources, comply with this order.

(2) Ensure that authorized users complete GSA's annual IT Security Awareness and Privacy 101Training when they first access GSA IT resources and annually thereafter.

(3) Coordinate and arrange system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization)

b. Authorized Users: Must use GSA IT resources in an ethical and lawful manner and comply with the IT General Rules of Behavior and the federal and GSA policies referenced in this order.

c. GSA Authorizing Officials (AOs) must establish appropriate system/organization-unique rules of behavior for systems under their authority.

8. Penalties for non-compliance. Users who do not comply with the IT General Rules of Behavior may incur disciplinary action, as well as civil and criminal liability.

9. IT General Rules of Behavior.

Category	Rules of Behavior
Personal Use	While GSA provides IT resources for official use, GSA does authorize users to utilize email and social media and access the Internet for personal use provided that users keep the use and access to a minimum and do not interfere with official system use or access. Users must not use IT resources for their own or others private gain, commercial purposes (including endorsement), or profit-making activities.
Privacy	(1) Users have no expectation of privacy on GSA IT resources since all activities are subject to monitoring. (2) Take measures to protect Personally Identifiable Information (PII) and sensitive data, as described in GSA Order CIO P 2180.1, to include use of encryption, access controls, data extracts, and physical security.
Protection	Protect GSA IT resources from theft, destruction, or misuse as described in this order.
Access	(1) Maintain the confidentiality of passwords; do not share passwords with anyone, including other employees, management, or technical personnel; and do not write, display, or store passwords where others may access or view them. (2) Do not attempt unauthorized access to an IT resource, including information contained in any system or application. (3) Lock GSA systems with a PIN/password and remove PIV card when away from the work area, including for lunch, breaks, or any extended period of time. (4) Logoff and shutdown GSA systems at the end of the workday.
Antivirus protection	Do not interfere with GSA provided antivirus protection on GSA IT resources and provide and maintain up-to-date antivirus protection software on personally owned resources that access the GSA network.

Category	Rules of Behavior
Encryption	Use GSA provided encryption when storing, processing, or transmitting Personally Identifiable Information (PII) and/or sensitive data.
Hardware and Software	(1) Abide by software copyright laws and do not obtain, install, replicate, or use unlicensed software. (2) Obtain all software in coordination with the local help desk and the appropriate ISSO. Do not download software from the Internet, as downloading software from the Internet may introduce malware [1]to the GSA network. (3) Do not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.
Remote access	(1) Use only authorized mechanisms, such as, GSA provided VPN, Citrix, and https://email.gsa.gov, to remotely access the GSA network. (2) Do not connect to other networks (like your home network) or devices on other networks (like your home wireless printer) while connected to GSA network using VPN (split tunneling is not permitted). You should consider using a wired printer when using VPN and needing to print files. (3) Keep operating system and antivirus software up-to-date and maintain personal firewalls on devices used to access the GSA network.

[1] Malware is harmful software, such as, viruses or Trojans designed to cause damage or disruption to a computer system

Category	Rules of Behavior
Mobile devices and Mobile Applications	For laptops, tablets, smart phones, and other mobile devices: (1) Pay special attention to the protection of mobile devices to prevent loss or theft as well as the requirement for the use of encryption of PII or sensitive data. (2) Disable Bluetooth and Wi-Fi when not in use. (3) Prior to utilizing personally owned mobile devices to access the GSA network obtain approval from the Regional IT Manager, sign the GSA Personnel Device Usage Agreement, and receive a certification of device preparedness from IT Service Desk. Personally owned mobile devices must meet a number of requirements for passwords, lockout time, wipe capability, encryption, and other requirements. (4) Download apps only from trusted sources. (5) Get prior approval for applications that require the use of GSA network credentials to operate and applications that download, store or transmit GSA data on mobile devices.
Prohibited usage	(1) Never convey classified data or information over the GSA network. (2) Never convey any material that is sexually explicit, offensive, abusive, discriminatory or objectionable or browse sexually explicit or hate-based web sites. (3) Never transmit non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally send malware. (4) Never use copyrighted or otherwise legally protected material without permission. (5) Never use GSA IT resources to "snoop" on or invade another person's privacy or break into any computer, whether belonging to GSA or another organization. (6) Never transmit any material that is libelous or defamatory. (7) Never automatically forward GSA email to non-Federal email accounts or addresses

Category	Rules of Behavior
Security Awareness Training	Complete IT security awareness training when initially accessing GSA IT resources and annually thereafter
Reporting	Promptly report, to the appropriate Information Systems Security Officer (ISSO), and/or IT Service Desk, any observed or suspected security problems/ incidents, including loss/theft of IT resources, including PII, or persons requesting that you reveal your password.

10. Deviations.

Coordinate any deviations from this order with the appropriate ISSO and AO, who will notify the GSA Senior Agency Information Security Official (SAISO)."

11. Signature.

/S/
DAVID SHIVE
Chief Information Officer
Office of GSA IT